BIAŁA KSIĘGA

Cyfryzacja i cyberbezpieczeństwo w kontekście fizycznej kontroli dostępu

Studium poświęcone systemom i protokołom, które umożliwiają przedsiębiorstwom wykorzystywanie kontroli dostępu w maksymalnym stopniu i tworzenie inteligentniejszego, bezpieczniejszego świata

Sierpień 2021

AXIS COMMUNICATIONS

Spis treści

1 Streszczenie

Rozwój technologii chmury zmienia oblicze sektora bezpieczeństwa fizycznego i zmusza instalatorów, którzy chcą utrzymać się na rynku, do adaptacji. Wszystko wskazuje na to, że kontrolę nad systemami dostępu przejmują globalne firmy technologiczne. Systemy te stają się coraz inteligentniejsze, bardziej skalowalne i działają w środowisku brzegowym, w związku z czym rosną stawiane im oczekiwania.

Zjawisko to — oraz towarzysząca mu potencjalna możliwość integracji z innymi systemami korporacyjnymi — oznacza też, że podczas tworzenia i wdrażania systemów kwestia cyberbezpieczeństwa odgrywa jeszcze większą rolę. To znamienne zwłaszcza wówczas, gdy punkt wyjścia stanowi dotychczas istniejąca infrastruktura. Przezwyciężenie barier technicznych, takich jak architektura szeregowa czy brak adresów MAC, stanowi kluczowy etap przejścia ku cyfrowym systemom kontroli dostępu odpowiadającym zarówno na bieżące, jak i przyszłe potrzeby.

Implementacja i ochrona cyfrowego systemu kontroli dostępu wymaga również stosowania najlepszych praktyk, które pozwalają osiągnąć możliwie najwyższy poziom bezpieczeństwa. Należy oceniać i testować każdy komponent systemu — urządzenia, dostawców i protokoły — pod kątem ich wiarygodności i niezawodności. Ponadto trzeba nieprzerwanie obserwować aktualne zagrożenia i poszukiwać sposobów niwelowania tych, które towarzyszą nowo wykrywanym lukom i słabym punktom zabezpieczeń.

Na szczególną uwagę zasługują dostawcy, których urządzenia zostają dopuszczone do sieci przedsiębiorstwa. Dostawca, który chce być traktowany poważnie, powinien przygotować i udostępnić własne procedury zabezpieczania oferowanych rozwiązań. Przykładowo może opublikować przewodnik po zabezpieczeniach lub opracować specjalistyczne narzędzia upraszczające nadzorowanie i zabezpieczanie urządzeń sieciowych. Co więcej, dostawca powinien otwarcie i szczerze rozmawiać o swojej strategii działania w przypadku wykrycia luk i słabych punktów.

2 Wprowadzenie: przyszłość kontroli dostępu

Technologia chmury zrewolucjonizowała podejście do wdrażania i eksploatowania systemów, które do tej pory obowiązywało w dziedzinie bezpieczeństwa fizycznego. Użytkownicy końcowi i klienci oczekują inteligentniejszych, zintegrowanych i w większym stopniu ukierunkowanych biznesowo rozwiązań, które oferują możliwości dozoru i kontroli dostępu sięgające o wiele dalej niż te bazujące na tradycyjnych i nieco przestarzałych już technologiach.

Wielu dostawców stworzyło solidny model biznesowy oparty na fachowej wiedzy, usługach i znajomości różnych zagadnień w zakresie bezpieczeństwa fizycznego. Jednak sieci i internet rzeczy (IoT) ciągle ewoluują, co wymaga od przywiązanych do „tradycji" dostawców i montażystów zabezpieczeń fizycznych nauczenia się języka sfery IT — mówiącego o otwartych platformach, łączności IP i integracji oprogramowania. To konieczne, jeśli chcą przystosować się do zmiennych warunków rynkowych i utrzymać wypracowaną pozycję.

Wygląda na to, że jesteśmy świadkami błyskawicznego transferu szeroko rozumianej „kontroli". Z rąk dostawców elektronicznych systemów dostępu przejmują ją globalne korporacje technologiczne, które obecnie są w stanie nadawać nowy kształt branży bezpieczeństwa, wywracając ją do góry nogami. Inteligentne budynki i miasta otwierają pole ogromnych możliwości. Wielu ekspertów przewiduje dynamiczny rozwój dzisiejszego rynku systemów kontroli dostępu, argumentując to mnóstwem korzyści, jakie łatwość wdrażania i wyrafinowanie nowoczesnych technologii przynosi inteligentnemu środowisku.

Podczas globalnej pandemii COVID-19 chmura okazała się niezastąpiona. Nic więc dziwnego, że sukcesowi technologii chmurowych — znajdującemu potwierdzenie wśród technologicznych gigantów — towarzyszy dążenie ku zdalnym systemom kontroli dostępu. Korporacje dysponują zasięgiem, środkami i potencjałem pozwalającymi na przeprowadzenie radykalnej zmiany. Obejmie ona także sferę bezpieczeństwa fizycznego,

jako że przedsiębiorstwa dostrzegające wartość chmury poszukują zdalnych rozwiązań, mających odpowiadać za wszystkie kwestie związane z bezpieczeństwem i biznesem.

Obecnie jednak wielu producentów zwyczajnie nie jest jeszcze przygotowanych na nowe uwarunkowania rynkowe — nadal realizują oni modele biznesowe oparte na sztywnych, autorskich rozwiązaniach. Dążenie ku inteligentnym rozwiązaniom w dziedzinie bezpieczeństwa fizycznego stoi w zdecydowanym kontraście z tradycyjną strategią działania, która najprawdopodobniej zostanie gruntownie zweryfikowana. Zmiana nie nastąpi z dnia na dzień, a zdalnym rozwiązaniom chmurowym wciąż daleko do wiodących. Jednak taka właśnie wizja nowego, lepszego świata przyświeca wchodzącym do naszej branży młodym inżynierom.

Wszystko to oznacza, że kontrola dostępu, jak i cały sektor bezpieczeństwa fizycznego, zmierzy się w przyszłości z dużymi oczekiwaniami. Systemy kontroli dostępu zamienią się w punkty gromadzenia danych, a kontrolery drzwi — w inteligentne urządzenia we/wy. Kody QR do obsługi odwiedzających czy biometryczna technologia rozpoznawania twarzy, zapewniająca bezobsługowy dostęp, będą coraz częściej zarządzane w środowisku brzegowym w ramach analiz przeprowadzanych bezpośrednio w kamerze lub czujniku. Przyszłość kontroli dostępu rysuje się jako fascynujący, pełen wyzwań okres dla tych wszystkich, którzy się z nią pogodzą i pomogą ją kształtować. To prawdziwa okazja, by stworzyć innowacje na miarę inteligentniejszego i bezpieczniejszego świata.

W niniejszym artykule przyglądamy się kwestiom szczególnie ważnym z perspektywy kontroli dostępu, a także wielu podstawowym funkcjom tego rodzaju systemów. Omówimy najlepsze praktyki, którymi powinni kierować się dostawcy, a także podzielimy się ważnymi informacjami i wskazówkami z użytkownikami końcowymi. Dzięki temu zyskają większą pewność podczas kontaktów z dostawcami i będą podejmować lepiej przemyślane decyzje zakupowe.

3 Wyzwania w obliczu wciąż zmieniającego się rynku systemów kontroli dostępu

Jeśli chodzi o systemy fizycznej kontroli dostępu (Physical Access Control System — PACS), reagowanie na czynniki ryzyka zwykle rozpatruje się jako umożliwianie lub blokowanie fizycznego wejścia. System fizycznej kontroli dostępu należy przede wszystkim zaprojektować w przemyślany i racjonalny sposób, wychodząc od oceny potencjalnego zagrożenia.

Obecnie środowiska lokalne firm są chronione przez coraz bardziej zaawansowane elektroniczne rozwiązania kontrolujące dostęp. Systemy te pozwalają w szybki i skuteczny sposób nadzorować dostęp w każdym obszarze przedsiębiorstwa. Pozostawiają za sobą cyfrowy ślad, który w razie potrzeby można analizować i monitorować, a także w pełni współpracują z innymi systemami, na przykład do zarządzania HR i gośćmi.

Ujednolicenie systemów daje dostęp do wielu cennych informacji, które ułatwiają podejmowanie decyzji dotyczących bezpieczeństwa i działalności biznesowej, a także kontrolowanie dostępu. W związku z tym dokładna analiza cyberdojrzałości systemu zaczyna odgrywać niezwykle istotną rolę. Zapobieganie użyciu sklonowanych uprawnień dostępu, zagrożeniom wewnętrznym i zdalnym cyberatakom jest sporym wyzwaniem, ponieważ przestępcy działają w coraz bardziej wyrafinowany sposób, a zagrożenia nieustannie ewoluują.

Źródłem problemu jest jednak także sama architektura. Wiele tradycyjnych systemów kontroli dostępu opiera się na przestarzałej infrastrukturze. Integracja różnych technologii bezpieczeństwa, które powszechnie wykorzystują taką infrastrukturę, jest dla dostawców problematyczna. Z jednej strony wynika to z konieczności dostosowania platform sprzętowych do sieci firmowych, a z drugiej — z braku zrozumienia wagi bezpieczeństwa IT i zmian zachodzących na rynku zabezpieczeń oraz związanej z tym potrzeby dogłębnej analizy zagrożeń dla przedsiębiorstwa i ochrony przed nimi.

Cyberbezpieczeństwo powinno mieć kluczowe znaczenie podczas przygotowywania nowych systemów zabezpieczeń. Rozwiązania do kontroli dostępu są nieodłączną częścią wszystkich systemów zapewniania bezpieczeństwa fizycznego. Powinny być produkowane zgodnie z uznanymi zasadami cyberochrony i zgłaszania incydentów oraz najlepszymi praktykami. Należy mieć przy tym świadomość, że integralność systemu jest tak trwała jak jego najsłabsze ogniwo. **System, którego twórcy o tym zapomnieli**, może być narażony na ataki. Jeśli nie jest on w stanie akceptować i realizować powszechnie przyjętych działań naprawczych ani dostarczać informacji potrzebnych do ich wykonania, jego zdolność do zapewnienia wymaganego poziomu bezpieczeństwa fizycznego, z myślą o którym został wdrożony, jest mocno ograniczona.

3.1 Certyfikaty cyberbezpieczeństwa (cyberdojrzałość)

Rosnące zaangażowanie sektora IT powoli zaczyna zmieniać sposób, w jaki ocenia się, wdraża i uaktualnia rozwiązania techniczne. Dla partnera z branży IT kluczowe znaczenia ma ocena wiarygodności firmy pod kątem cyberbezpieczeństwa, a w szczególności wiedzy, jaką dysponuje na ten temat sprzedawca. Ta wiedza jest także nazywana cyberdojrzałością. Cyberdojrzałość sugeruje dobrą orientację w aktualnych zagrożeniach i sposobach ograniczania ryzyka. Opracowano już wiele dokumentów i wytycznych dotyczących kamer sieciowych. Zasoby te można odnieść także do fizycznej kontroli dostępu, ponieważ wyzwania, oceny i wyjaśnienia związane z cyberzagrożeniami i możliwością ataku są przydatne w przypadku obu tych rodzajów produktów.

3.2 Przyszłość architektury systemów bezpieczeństwa

Nowoczesne urządzenia do kontroli dostępu są połączone ze sobą za pomocą przewodów sieciowych i złączy RJ45. Sieci służą do zasilania kontrolerów dostępu, a także do komunikacji między urządzeniami i systemami centralnego zarządzania. Motorem rozwoju rozwiązań do kontroli dostępu okazało się przejście na systemy oparte na protokole TCP/IP. Od 2013 roku, gdy pojawił się pierwszy kontroler drzwi w pełni obsługujący protokół IP (AXIS A1001), systemy fizycznej kontroli dostępu wciąż są rozwijane. Dzisiejsze rozwiązania mają wiele zaawansowanych funkcji, które nie miałyby racji bytu, gdyby zastosowano w nich tylko starsze technologie.

Wśród wprowadzonych innowacji warto wymienić czytniki kodów QR, które ułatwiają bezdotykową kontrolę dostępu, mechanizmy rozpoznawania twarzy zintegrowane z kamerami sieciowymi i czytniki tablic rejestracyjnych. Wszystkie te rozwiązania współdziałają z bazami danych PACS, dzięki czemu decyzje o udzieleniu lub odmowie dostępu są podejmowane na brzegu sieci. Do najważniejszych zalet systemów IP należą niskie koszty instalacji oraz łatwa konfiguracja i proste zarządzanie urządzeniami. Bezproblemowa integracja z innymi urządzeniami pozwala na tworzenie rozwiązań, które sprawdzą się także w przyszłości i będą współpracować z nowymi zabezpieczeniami i udoskonaleniami od razu po ich udostępnieniu.

3.3 Technologia IP a tradycyjna kontrola dostępu

Protokół IP jest naturalną platformą dla nowoczesnych systemów kontroli dostępu, w szczególności tych bezkontaktowych, których dziś oczekują użytkownicy. Użytkownicy będą też oczekiwać tego, by mechanizmy kontroli dostępu działały na smartfonach oraz tabletach i to nie tylko na bazie uwierzytelniania mobilnego. Co zrobić, by dostarczać lepsze, bardziej przydatne, szybsze i tańsze systemy kontroli dostępu? Jak nadążyć za tempem innowacji narzucanym przez gigantów technologicznych? Oto pytania, na które dostawcy muszą znaleźć odpowiedź, by utrzymać się na rynku.

Jak dotąd kwestie te pozostają nierozwiązane. Wynika to zapewne z tego, że starsze systemy kontroli dostępu opierają się na kontrolerach drzwi instalowanych w architekturze szeregowej i połączonych

z jednostką centralną lub serwerem za pomocą interfejsu przewodowego RS-485. Ponadto większość systemów to rozwiązania zastrzeżone, co oznacza, że kontrolerem drzwi można zarządzać jedynie za pomocą oprogramowania dopuszczonego przez dostawcę. Z tego powodu użytkownik jest ograniczony do sprzętu i oprogramowania od jednego dostawcy, a złożoność takich systemów sprawia, że ich instalację i skonfigurowanie trzeba powierzyć personelowi zewnętrznemu.

Rozbudowa tradycyjnego systemu dostępu jest trudna, ponieważ standardowy sterownik centralny jest przeznaczony do obsługi określonej liczby drzwi. Tak nieduża elastyczność sprawia, że wdrażanie nietypowych konfiguracji jest bardzo kosztowne. Nawet dodanie jednych dodatkowych drzwi może znacząco podnieść koszty, przez co inwestycja traci na opłacalności.

Sieci IP pozwalają na wdrożenie o wiele prostszej i łatwej w instalacji architektury PACS, która ma dużo większą elastyczność i szersze możliwości dostosowania. Specjaliści IT wyraźnie preferują urządzenia w pełni oparte na technologii IP i wykorzystują je w sieciowych systemach kontroli dostępu. Włączenie takich fachowców do procesu projektowania jest niezwykle ważne, ponieważ zadbają oni o wdrożenie urządzeń IP, które są kluczem do ograniczenia kosztów rozbudowy i będą potrzebne w systemach kontroli dostępu instalowanych w przyszłości.

3.4 Protokoły otwarte

Przyszłość kontroli dostępu zależy od tego, czy producenci będą chcieli dzielić się swoimi umiejętnościami i zasobami w ramach protokołów otwartych. Powody niechęci do tej otwartości są oczywiste. Wielu twórców systemów woli rozwiązania, w których użytkownik końcowy jest przywiązany do jednego dostawcy, ponieważ mają dzięki temu pewny dochód w przyszłości. Korzyści tej strategii są jednak krótkotrwałe. Użytkownicy oczekują od rozwiązań coraz więcej, dlatego chętnie dzielą się ze sobą danymi, które pomagają osiągnąć ten cel.

Projektanci systemów i dostawcy sprzętowych zabezpieczeń dostępu rzadko dysponują zasobami lub zapleczem IT, które pozwalałyby im oferować użytkownikom wszystkie rozwiązania potrzebne do stworzenia systemu bezpieczeństwa fizycznego. Wielu dostawców wydaje się nie rozumieć, że ich produkty są szybko wypierane przez nowe, innowacyjne rozwiązania, które zagrażają zarówno ich modelowi biznesowemu, jak i pozycji na rynku rozwiązań kontroli dostępu. Możliwości najnowszych systemów i szybkość nowoczesnych, innowacyjnych rozwiązań są tak duże, że już niedługo kontrolery dostępu staną się zbędne, ponieważ w naturalny sposób zastąpią je inteligentne jednostki we/wy.

Rozwiązania otwarte pozwalają dostawcom tworzyć urządzenia odpowiednie dla niewielkich systemów, w przypadku których kluczową rolę odgrywa prostota oraz koszt zakupu i instalacji. Takie urządzenia można później w razie potrzeby dostosować do zadań o większej skali i bardziej zaawansowanych technicznie. Nowoczesne systemy bezpieczeństwa charakteryzuje elastyczność, dzięki czemu rozwiązania kupione dziś będą użyteczne także w przyszłości, gdy zmienią się wymagania użytkownika, a jego działalność się rozrośnie.

Więcej informacji o podejściu i technologiach otwartych można znaleźć na stronie internetowej ONVIF *www.onvif.org* — organizacji branżowej, która działa na rzecz rozwoju technologii otwartych.

4 Techniczne przeszkody we wdrożeniu

Na działanie cyfrowego systemu kontroli dostępu składa się wiele elementów związanych z połączeniami technicznymi, interfejsami i urządzeniami. Przejście z systemów tradycyjnych na rozwiązania działające w chmurze może rodzić wiele problemów. W dalszych częściach omówiono te aspekty, które należy uwzględnić, by dotychczasowe rozwiązania i związane z nimi procesy były przydatne i nie stanowiły bariery utrudniającej modernizację i wdrożenie nowych rozwiązań.

4.1 Sterowniki RS-485

Jedną z problematycznych kwestii jest wdrożenie sterowników RS-485 i potencjalne ryzyko instalacji urządzeń semiinteligentnych, które rzadko, o ile kiedykolwiek, mają adres MAC (ang. media access control), przez co są trudne do zidentyfikowania. RS-485 (lub TIA-485(-A) bądź EIA-485) to standard określający charakterystykę elektryczną sterowników i odbiorników używanych w szeregowych systemach komunikacji. Mechanizm sygnalizacji elektronicznej jest zrównoważony i obsługiwane są systemy wielopunktowe. Standard RS-485 dotyczy tylko warstwy fizycznej, czyli generatora i odbiornika i nie odpowiada za kluczową warstwę komunikacyjną.

Trzeba jednak zauważyć, że brak adresu MAC lub implementacja architektury szeregowej nie muszą oznaczać problemów z niezawodnością lub nieprawidłowego działania systemu kontroli dostępu. W końcu systemy te z powodzeniem opierały się na takich rozwiązaniach przez ponad 30 lat. Trudno sobie jednak wyobrazić, by można było wychodzić naprzeciw nowoczesnym potrzebom w zakresie bezpieczeństwa bez systemu kontroli, w którym każde urządzenie kontrolujące jest inteligentne i może mieć oddzielny adres. Naszym zdaniem tylko prawdziwie inteligentne systemy i w pełni dostępne urządzenia będą mogły sprostać przyszłym wyzwaniom w zakresie ochrony. „W pełni dostępne" nie oznacza przy tym, że takie urządzenia nie są skutecznie chronione przed cyberzagrożeniami. Wręcz przeciwnie.

4.1.1 Protokół OSDP (ang. Open Supervised Device Protocol)

Protokół OSDP (ang. Open Supervised Device Protocol) to nowe rozwiązanie komunikacyjne zaakceptowane przez IEC. Umożliwia on zwiększenie bezpieczeństwa komunikacji w ramach systemów kontroli dostępu i został przygotowany przez organizację Security Industry Association (SIA) w celu zwiększenia wzajemnej kompatybilności rozwiązań w dziedzinie bezpieczeństwa i kontroli dostępu. Protokół OSDP wykorzystuje szyfrowanie 128-bitowe, obsługuje instalacje wielopunktowe i nadzoruje połączenia celem zgłaszania problemów z czytnikami. Oprócz tego protokół OSDP obsługuje czytniki kart, elektrozaczepy, styki alarmowe i funkcje wyjścia (request to exit), przy czym potrzebuje do tego tylko dwóch przewodów zamiast wielu punktów połączonych z każdymi drzwiami, jak wymagano wcześniej. Na stronie internetowej SIA można przeczytać, że „protokół OSDP został zatwierdzony jako standard międzynarodowy przez Międzynarodową Komisję Elektrotechniczną w maju 2020 roku, a dotyczącą tego rozwiązania normę IEC 60839-11-5 opublikowano w lipcu 2020 roku. Protokół OSDP autorstwa SIA jest ciągle doskonalony, by pozostawał najlepszym rozwiązaniem tego typu na rynku".

4.2 Zalety urządzeń z adresem MAC

Adres MAC jest unikalnym w skali globalnej adresem sprzętowym pojedynczego urządzania lub adaptera sieciowego. Gdy chodzi o sieć IT, adres MAC jest równie ważny, jak adres IP. Adres MAC jednoznacznie identyfikuje komputer w sieci LAN i jest potrzebny do funkcjonowania protokołów sieciowych, takich jak TCP/IP. Jest on niezmienny dla urządzenia i choć można go ominąć za pośrednictwem systemu operacyjnego, nie należy tego robić, ponieważ adres powinien być chroniony zabezpieczeniami.

Technologia TCP/IP i inne popularne architektury sieciowe opierają się zazwyczaj na modelu OSI (ang. Open Systems Interconnection), w którym system sieciowy dzieli się na warstwy. Adresy MAC należą do warstwy łącza danych (warstwy 2. w modelu OSI) i pozwalają na jednoznaczną identyfikację komputerów w sieci. Filtrowanie adresów MAC zapewnia z kolei dodatkową warstwę ochrony. Przed zezwoleniem na dołączenie urządzenia do sieci router sprawdza, czy jego adres MAC znajduje się na liście zatwierdzonych adresów. Dostęp jest przyznawany tylko wtedy, gdy adres klienta znajduje się na liście routera.

4.2.1 Zasilanie przez sieć Ethernet (PoE)

Oszczędność i elastyczność w rozmieszczeniu urządzeń to dwie korzyści, jakie zapewnia technologia PoE (ang. Power over Ethernet), niezależnie od zastosowania. Technologia PoE pozwala na przesyłanie danych i zasilania tym samym przewodem, co oznacza, że architektura urządzeń może być prostsza niż w tradycyjnych systemach. Warto też zauważyć, że wiele systemów kontroli dostępu jest promowanych jako podłączone do sieci IP.

5 Cechy charakterystyczne najlepszych praktyk

Zarządzanie kontrolą dostępu jest ważną częścią skutecznego nadzorowania przepływu ludzi i wykorzystania dostępu. Zamykanie drzwi i stawianie szlabanów to za mało. Firmy potrzebują lepszych możliwości kontroli, by przez cały czas zapewniać klientom lepszą obsługę i wyższy poziom bezpieczeństwa, W zapewnieniu kompleksowej ochrony zgodnie z najlepszymi praktykami chodzi o coś więcej niż tylko wybranie odpowiednich narzędzi. Potrzebna jest też właściwa architektura, implementacja technologii wysokiej jakości, przestrzeganie stosownych procedur i protokołów, a także zachęcenie personelu i partnerów do prezentowania prawidłowych postaw i zachowań.

5.1 Zarządzanie interesariuszami i konwergentne podejście do bezpieczeństwa

Ekosystem technologii w ramach tej samej infrastruktury jest coraz lepiej zintegrowany, dzięki czemu dostępne są rozwiązania operacyjne potrzebne do bezproblemowego funkcjonowania. Dlatego też proces podejmowania decyzji również musi być spójny. Można już wymienić kilka przykładów, w których konwergentne podejście do bezpieczeństwa pozwoliło zburzyć mury między rożnymi zespołami i zacząć im ze sobą współpracować. Konwergencja jeszcze nigdy nie była tak ważna jak dziś, gdy tradycyjne produkty do ochrony elektronicznej i fizycznej funkcjonują obok sieci firmowych.

Zespoły zajmujące się bezpieczeństwem fizycznym muszą korzystać z technologii służących realizacji wymogów operacyjnych i zapobieganiu powiązanym zagrożeniom. Technologie te powinny jednocześnie pozwalać na stosowanie się do zasad bezpieczeństwa IT i zapobieganie atakom na sieć firmową podejmowanym za pośrednictwem urządzeń fizycznych. Współpraca wszystkich partnerów pozwala na stworzenie bezpiecznego środowiska cyfrowego i fizycznego.

5.2 Czego oczekiwać od partnerów, sprzedawców i dostawców

To ważne, by podmioty zewnętrzne rozumiały, jak istotne jest stosowanie najlepszych praktyk bezpieczeństwa we wszystkim, co robią, a przy tym działały tak, by realizować konkretne potrzeby. Relacje z podmiotami zewnętrznymi są bardzo ważne dla zbudowania zdrowego łańcucha dostaw oraz trwałych i opartych na zaufaniu powiązań.

Najistotniejsze aspekty, które należy uwzględnić w ocenie podmiotów zewnętrznych i ich wpływu na łańcuch dostaw:

- Podmiot rozumie i przyjmuje do wiadomości czynniki ryzyka związane z cyberbezpieczeństwem
- Podmiot potrafi wykazać dojrzałe podejście do cyberbezpieczeństwa z uwzględnieniem dostępnych procesów i narzędzi
- Podmiot rozumie wpływ regulacji i ustawodawstwa na swoją ofertę
- Podmiot potrafi wykazać, jak będzie wspierać użytkownika w spełnianiu wymagań prawnych

- Cyberzabezpieczenia to nie tylko technologia, ale i proces — podmiot potrafi zaprezentować zarządzanie cyklem istnienia cyberzabezpieczeń z myślą o ochronie przedsiębiorstwa użytkownika.

5.3 Zarządzanie zabezpieczeniami: procesy dotyczące nadzoru i obsługi sprzedawców

Poziom cyberbezpieczeństwa, tak jak i każdego innego rodzaju bezpieczeństwa, zależy od gruntowności zabezpieczeń. Kluczem jest tu odpowiednia ochrona sieci kamer IP na każdym poziomie — od wybranych produktów i partnerów po określone wymagania.

5.3.1 Normy i rozporządzenia

Norma ISO/IEC 27001 dotycząca Systemów Zarządzania Bezpieczeństwem Informacji określa wymagania dotyczące systemów zarządzania bezpieczeństwem, takie jak:

- Systematyczne analizowanie ryzyka dotyczącego bezpieczeństwa informacji w organizacji przy uwzględnieniu zagrożeń, ich konsekwencji i luk w zabezpieczeniach.
- Zaprojektowanie i wdrożenie spójnego, kompleksowego zestawu środków ochrony informacji i/lub innych form zarządzania ryzykiem (takich jak unikanie i przenoszenie ryzyka), by ograniczyć zagrożenia, które wydają się niedopuszczalne.
- Wdrożenie całościowego procesu zarządzania w celu utrzymania pracy systemów kontroli bezpieczeństwa, by na bieżąco zaspokajać potrzeby przedsiębiorstwa w zakresie bezpieczeństwa informacji.

5.3.2 Cyber Essentials Plus

Cyber Essentials to wspierany przez rząd i instytucje branżowe program certyfikacji, który pomaga organizacjom chronić się pod powszechnymi zagrożeniami internetowymi. Certyfikat Cyber Essentials to dobry wyznacznik tego, czy firma rozumie wyzwania związane z cyberbezpieczeństwem. Pozwala na ewaluację procesów i zasad obowiązujących w organizacji. Aspekty, na których skupia się program:

- Bezpieczeństwo konfiguracji
- Kontrola dostępu i administracja
- Ochrona przed szkodliwym oprogramowaniem
- Zarządzanie poprawkami
- Zapora i bramy internetowe

Dla producentów rozwiązań technicznych pierwszą linią obrony powinny być środki ograniczające ryzyko zagrażające ich własnym systemom. Od 1 października 2014 roku rząd wymaga, by dostawcy uczestniczący w przetargach o kontrakty obejmujące przetwarzanie danych wrażliwych i osobowych przechodzili proces certyfikacji Cyber Essentials.

5.3.3 Domyślne bezpieczeństwo od etapu projektowania (ang. Secure by Design, Secure by Default)

W 2019 roku brytyjski komisarz ds. monitoringu wizyjnego opublikował wytyczne **Secure by Design, Secure by Default**, w których określono minimalne wymagania stawiane producentom systemów i podzespołów kamer dozorowych. Od producentów oczekuje się między innymi holistycznego rozwiązywania problemów i zajmowania się główną przyczyną zamiast jej widocznymi skutkami oraz podejmowania działań proporcjonalnych do potrzeb, tak by ograniczyć całkowite szkody w systemie lub danym podzespole.

W wytycznych Secure by Design, Secure by Default przedstawiono również długoterminowe środki techniczne, które dają pewność, że w sprzęt i oprogramowanie wbudowano właściwe zabezpieczenia podstawowe. W dokumencie omówiono też inne równie wymagające zadanie jakim jest dbanie o dostępność i funkcjonalność zabezpieczeń, dzięki czemu użytkownicy mogliby od razu zacząć je wdrażać.

Ponieważ jako Axis chcemy, by nasze technologie były lepsze, połączyliśmy wytyczne Secure by Design, Secure by Default z założeniami kodeksu postępowania określonymi w krajowej strategii cyberbezpieczeństwa (National Cybersecurity Strategy):

- Monit o hasło
- Wskaźnik siły hasła
- Szyfracja HTTPS
- 802.1x
- WYŁĄCZONY dostęp zdalny (trawersowanie NAT)

6 Porady i narzędzia (procesy dotyczące sprzedawców)

Organizacje często decydują się na zabezpieczenie sieci oparte na kilku technicznych środkach kontroli, by uzyskać „wielowarstwowy system bezpieczeństwa", który ułatwia ograniczenie pojedynczych punktów awarii i narażenia. Nieraz zapominają jednak przy tym o „wzmocnieniu systemu", które polega na zmianie domyślnych ustawień systemu w celu ochrony informacji. Ponadto proces ten pomaga ograniczyć liczbę luk, które nieuchronnie występują w zabezpieczeniach każdego systemu.

6.1 Przewodnik dotyczący wzmacniania zabezpieczeń w produkcji

Wszystkie urządzenia podłączone do sieci powinny podlegać procesowi wzmacniania zabezpieczeń systemów. Dotyczy to stacji roboczych, serwerów i innych urządzeń sieciowych. Nikt nie zna konfiguracji systemu tak, jak jego producent, dlatego to on ma obowiązek dostarczyć partnerom i użytkownikom informacje potrzebne do ochrony integralności urządzeń i instalacji po stronie użytkownika końcowego. Porady techniczne dla wszystkich osób uczestniczących we wdrażaniu rozwiązań do nadzoru wizyjnego powinny znajdować się w przewodniku po wzmacnianiu zabezpieczeń. Porady te powinny obejmować opis bazowej konfiguracji, a także kompleksowe informacje na temat radzenia sobie z ewoluującymi zagrożeniami.

Wszyscy dostawcy powinny dokładać starań, by na etapie projektowania, tworzenia i testowania urządzeń stosować najlepsze standardy cyberbezpieczeństwa w celu zminimalizowania ryzyka wystąpienia wad, które mogłyby zostać wykorzystane do przeprowadzenia ataku. Ochrona sieci, należących do niej urządzeń i usług, które obsługuje, wymaga jednak czynnego zaangażowania wszystkich podmiotów w łańcuchu dostaw, a także organizacji będącej użytkownikiem końcowym. Bezpieczeństwo środowiska zależy od jego użytkowników, procesów i technologii. Dobry przewodnik powinien uwzględniać podstawowe problemy, takie jak te wymienione w dokumencie CIS Controls - Version 6.1. Jest to lista elementów wymagających skontrolowania znana wcześniej pod nazwą SANS Top 20 Critical Security Controls.

6.2 Zarządzanie urządzeniami

Menedżer urządzenia to narzędzie lokalne pozwalające na łatwe, ekonomiczne i bezpieczne zarządzanie skomunikowanymi urządzeniami. Za jego pomocą instalatorzy i administratorzy systemów mogą bardzo skutecznie zarządzać wszystkimi kluczowymi zadaniami związanymi z instalacją, bezpieczeństwem i konserwacją.

Ewidencja urządzeń / system zarządzania zasobami:

- Zasady dotyczące kont i haseł
- Sprawna instalacja aktualizacji oprogramowania sprzętowego/układowego i aplikacji
- Stosowanie zabezpieczeń przed cyberatakami — zarządzanie HTTPS, przesyłanie certyfikatów IEEE 802.1x, zarządzanie kontami i hasłami
- Zarządzanie cyklem życia certyfikatów — zarządzenie wszystkimi kluczowymi zadaniami dotyczącymi instalacji, bezpieczeństwa i eksploatacji
- Szybka, łatwa konfiguracja nowych urządzeń — kopia zapasowa i odtwarzanie ustawień
- Dla każdej lokalizacji niezależnie od rozmiaru — instalacja w jednej lub wielu lokalizacjach

6.3 Wyzwania związane z producentami OEM/ODM

Producent oryginalnego sprzętu (ang. original equipment manufacturer, OEM) odsprzedaje produkt innej firmy pod własną nazwą i marką. Producent oryginalnego projektu (ang. original design manufacturer, ODM) to firma projektująca i wytwarzająca produkt według specyfikacji innej firmy, która następnie sprzedaje go pod własną marką. Takie rozwiązania pozwalają markom na udział w produkcji bez uruchamiania i prowadzenia fabryki.

Wybór produktu OEM lub ODM innego dostawcy ma dla producenta wiele zalet. Po pierwsze uwalnia organizację od wszelkich zagrożeń i kosztów związanych z produkcją i pozwala jej skupić się na sprzedaży i procesach marketingowych. To jeden z głównych powodów, dla których wielu producentów kamer z sektora bezpieczeństwa decyduje się produkować sygnowane przez siebie produkty w modelu OEM lub ODM.

Niesie to za sobą kilka wyzwań, z których najbardziej oczywistym jest cyberbezpieczeństwo. Jeśli w zabezpieczeniach produktów od jednego dostawcy istnieje luka, może to mieć wpływ na innych odsprzedawców i partnerów w całym łańcuchu dostaw. Produkcja w takim modelu może znacznie utrudnić utrzymanie pełnej przejrzystości łańcucha dostaw. Jeśli w procesie uczestniczy wielu producentów OEM i ODM, może okazać się, że użytkownik końcowy, który na podstawie analizy due diligence odrzucił rozwiązania od konkretnego wytwórcy, nieświadomie i wbrew własnej woli kupił te same rozwiązania, ale pod inną marką.

6.4 Mikroprocesorowy układ scalony CPU

Standardowe układy CPU instalowane w urządzeniach mają wiele znanych luk w zabezpieczeniach i dlatego są często atakowane przez hakerów. Jedną z głównych przyczyn tej sytuacji jest skalowalność takich ataków, ponieważ do ich przeprowadzenia wystarczy zidentyfikowanie jednej luki w zabezpieczeniach. Do niedawnych przykładów takich ataków należy wykorzystanie luk „Meltdown" i „Spectre" do zaatakowania kanałem bocznym nowoczesnych mikroprocesorów CPU. Luki te pozwalają na nielegalne uzyskanie dostępu do danych za pomocą nieuprawnionego kodu.

Większość urządzeń — od smartfonów po sprzęt komputerowy w centrach przetwarzania danych — może być do pewnego stopnia podatna na zagrożenia. Sprzedawcy głównych systemów operacyjnych oferują poprawki, które minimalizują takie problemy, jednak niektóre części tych poprawek trzeba instalować za pośrednictwem producenta OEM, ponieważ zawierają one elementy specyficzne dla danej platformy. Organizacja National Cybersecurity Centre (NCSC) zaleca instalowanie poprawek na urządzeniach tak szybko, jak to możliwe.

6.5 Strategia dotycząca oprogramowania układowego

Podpisane oprogramowanie układowe jest ważne dla użytkowników końcowych i minimalizuje niektóre z potencjalnych zagrożeń dotyczących urządzeń podczas realizacji procesu logistycznego i/lub dystrybucji. Podpis, nazywany też skrótem (ang. hash), jest dodawany do oprogramowania układowego podczas jego dystrybucji. Procesor wylicza własny skrót i wczytuje tylko ten obraz oprogramowania układowego, który ma skrót odpowiadający skrótowi podpisanemu zaufanym certyfikatem.

6.6 Postępowanie z lukami w zabezpieczeniach

Ciągły rozwój cyberprzestępczości i związane z nim zagrożenia zmuszają wiele organizacji do przywiązywania większej wagi do bezpieczeństwa informacji. Zarządzanie lukami w zabezpieczeniach powinno być częścią realizowanej przez organizację strategii kontrolowania zagrożeń związanych z bezpieczeństwem informacji. Proces ten daje stały wgląd w luki w zabezpieczeniach w środowisku IT i związane z nimi zagrożenia. Jedynie identyfikowanie i minimalizowanie luk w zabezpieczeniach środowiska IT może uchronić organizację przed atakiem na jej sieci i kradzieżą informacji.

To niezwykle ważne, by działalność dostawców obejmowała zarządzanie lukami w zabezpieczeniach, w tym procesy wykrywania i naprawiania luk w zabezpieczeniach wszystkich systemów, a także zapobieganie powstawaniu nowych luk podczas wprowadzania zmian lub wdrażania nowych systemów. Wszystkie kwestie dotyczące ryzyka akceptowanego przez dostawcę muszą być komunikowane i uzgadniane z użytkownikiem końcowym. Jeśli ta zasada nie zostanie wdrożona, hakerzy mogą wykorzystywać luki w systemach do atakowania przedsiębiorstwa i jego dostawców.

Poprawki zabezpieczeń IT i aktualizacje dotyczące luk w zabezpieczeniach muszą być instalowane w odpowiednim czasie i w ramach zatwierdzonego procesu, by zapobiec naruszeniom zabezpieczeń. W systemach dostawcy, które nie mogą być aktualizowane i stają się podatne na ataki, należy stosować odpowiednie środki ochrony. Wszystkie zmiany należy wprowadzać zgodnie z wdrożonym przez dostawcę procesem zarządzania zmianą.

6.7 Powiadomienia z ostrzeżeniami dotyczącymi bezpieczeństwa

Ostrzeżenia dotyczące bezpieczeństwa pomagają zredukować ryzyko wynikające ze znanych luk w zabezpieczeniach. Ostrzeżenia dotyczące bezpieczeństwa mogą odnosić się do raportu CVE (ang. Common Vulnerability and Exposure — powszechne luki w zabezpieczeniach i źródła narażenia) oraz innych oficjalnych raportów na temat podatności na zagrożenia. Ponadto takie ostrzeżenia zawierają opis luk w zabezpieczeniach, ocenę ryzyka, zalecenia i informacje o dacie udostępnienia danej wersji usługi. Większość sprzedawców wdraża model sprzedaży pośredniej i prowadzi program partnerski.

Powiadomienia z ostrzeżeniami dotyczącymi bezpieczeństwa pozwalają klientom, którzy nie są zarejestrowani w programie partnerskim producenta, otrzymywać istotne powiadomienia w najwcześniejszym możliwym terminie i wtedy, gdy są one komunikowane w danym kanale. To kluczowe narzędzie dla użytkowników końcowych, którzy mają zainstalowany sprzęt, ale nie zawarli umowy z firmą odpowiedzialną za jego instalację.

6.8 Model BSIMM (ang. Building Security in Maturity Model)

BSIMM to system oceny zabezpieczeń oprogramowania stworzony, by pomagać organizacjom w porównywaniu swoich zabezpieczeń z innymi projektami i określaniu swojego poziomu bezpieczeństwa. Model BSIMM ułatwia analizowanie procesów, aktywności, ról i obowiązków dzięki:

- Weryfikacji projektów i architektury
- Weryfikacji kodu
- Testowaniu pod kątem znanych luk w zabezpieczeniach
- Uruchomieniu narzędzia do przeszukiwania standardowych luk w zabezpieczeniach, w tym błędów CVE w pakietach Open Source

6.9 Wsparcie długoterminowe (LTS)

Wsparcie długoterminowe to polityka zarządzania cyklem życia produktów, zgodnie z którą stabilna wersja oprogramowania jest obsługiwana dłużej niż wersja standardowa. Oprogramowanie układowe LTS powinno zawierać tylko te poprawki, które dotyczą stabilności, wydajności i bezpieczeństwa. Dostawcy udostępniają oprogramowanie układowe LTS nawet przez 10 lat od wprowadzenia urządzenia na rynek.

Zakłada się, że wsparcie LTS działa równolegle do już aktywnego wsparcia dla oprogramowania, ale niezależnie od niego. Jedną z najważniejszych zalet wsparcia LTS jest utrzymanie kompatybilności z rozwiązaniami zewnętrznymi dla oryginalnej wersji oprogramowania układowego.

6.10 Nauka i współpraca

Jednym z kluczowych aspektów, które należy uwzględnić, gdy wybiera się dostawcę technologii, jest jego oferta w zakresie przeszkolenia i wsparcia. Wyzwania związane z tym kanałem i branżą ciągle ewoluują, co szczególnie mocno widać w przypadku cyberbezpieczeństwa. Producenci powinni więc wykazywać proaktywną postawę w tym obszarze i oferować dodatkowe zabezpieczenia i przydatne treści. Przykładowe rozwiązania to:

- Bezpłatne, stacjonarne kursy dotyczące cyberbezpieczeństwa
- Szkolenia internetowe z cyberbezpieczeństwa
- Krótkie testy internetowe z cyberbezpieczeństwa
- Przewodnik dotyczący wzmacniania systemów
- Polityki dotyczące luk w zabezpieczeniach
- Najlepsze praktyki w zakresie cyberbezpieczeństwa
- Spis pojęć i terminów z zakresu cyberbezpieczeństwa

7 Dbanie o cyberhigienę: dalsze kroki i zalecenia

Dobra cyberhigiena polega na identyfikowaniu i ustalaniu wagi zagrożeń dotyczących kluczowych usług i produktów danej organizacji oraz reagowaniu na nie. Wdrożenie najlepszych praktyk w zakresie bezpieczeństwa i cyberhigieny pomaga zapobiegać naruszeniom zabezpieczeń danych i stosowaniu niewłaściwych konfiguracji systemu, a przy tym minimalizuje związane z tymi kwestiami zagrożenia

dla samej działalności. Ważne jest również, by uzgodnić z partnerami kluczowe zagrożenia i skupić się na najważniejszych celach zarządzania ryzykiem.

Poniżej przedstawiono listę wybranych zaleceń, których wdrożenie ułatwia skuteczną walkę z cyberzagrożeniami.

7.1 Dostawcy

Sprawdzanie rejestracji i certyfikatów

Weryfikacja rejestracji i certyfikatów, np. poprzez poproszenie o dowód otrzymania certyfikatu ISO9000 i innych zaświadczeń dotyczących jakości. Określenie, czy produkty dostawcy są przeznaczone do użytku w sieci firmowej.

Sprawdzenie zgodności z najlepszymi praktykami

Zweryfikowanie, czy dany dostawca może wykazać się stosowaniem najlepszych praktyk w zakresie bezpieczeństwa. Dostawca powinien oferować przewodnik dotyczący „wzmacniania zabezpieczeń" systemów, w którym opisane są środki ochrony fizycznej i cyfrowej oraz najlepsze praktyki w zakresie zabezpieczania sieci.

Przeprowadzenie audytu dostawcy

Przed zobowiązaniem się do zakupu należy przeprowadzić dokładny audyt. Należy sprawdzić warunki umowy i upewnić się, że są one zrozumiałe i przejrzyste. Ważne z perspektywy finansowej jest zapytanie o to, co stanie się z produktem i jego wsparciem, jeśli dana firma zacznie gorzej prosperować.

Zidentyfikowanie źródeł bieżącego wsparcia

Należy upewnić się, czy dostawca ma zasoby wymagane do dalszego tworzenia rozwiązań, które mogą być potrzebne użytkownikowi w przyszłości. Istotna jest weryfikacja, czy rozmiar, zasięg i możliwości dostawcy pozwolą mu na spełnienie potrzeb biznesowych klienta w przyszłości.

Określenie przyszłych potrzeb biznesowych

Warto pomyśleć o swoich przyszłych potrzebach. Inteligentne urządzenia i rozwiązania pozwalają na sprawniejsze prowadzenie działalności i przygotowanie jej na przyszłe wyzwania, dlatego należy mieć pewność, że wybrany dostawca będzie spełniał, a nawet przekraczał, oczekiwania klienta, wywiązywał się z umów dotyczących konserwacji oraz zapewniał bieżące wsparcie.

Sprawdzenie, czy działalność jest prowadzona etycznie

Należy sprawdzić, czy dostawca prowadzi działalność w sposób etyczny i zrównoważony. Partnerstwo oparte na zaufaniu i wspólnych celach jest ważne dla długotrwałej współpracy. Czy dostawca wdrożył systemy zarządzania środowiskiem, program CSR (ang. corporate social responsibility — społeczna odpowiedzialność przedsiębiorstw) lub politykę etycznego pozyskiwania zasobów?

7.2 Produkty i systemy

Przeprowadzenie analizy due diligence

Analiza techniczna due diligence systemu i jego kluczowych elementów pozwala upewnić się, że jest on wartościowym rozwiązaniem i nie istnieją żadne czynniki wyjściowe, które mogłyby wpłynąć na ciągłość funkcjonowania. Informacje o analizie ryzyka i jego ograniczaniu muszą być jasne i dostępne.

Sprawdzenie umowy dotyczącej konserwacji

Należy sprawdzić, co wchodzi w zakres umowy. Trzeba na przykład wiedzieć, czy umowa dotycząca obsługi i konserwacji obejmuje też aktualizację oprogramowania producenta i nowe wersje oprogramowania układowego.

Zabezpieczenie skomunikowanych urządzeń

Należy zadbać o ochronę fizycznego systemu bezpieczeństwa, który jest podłączony do sieci. Przy implementacji systemu zabezpieczeń należy pamiętać o cyberbezpieczeństwie: zmienić domyślne hasło i nazwę użytkownika, zainstalować najnowsze oprogramowanie układowe, korzystać z szyfrowania (najlepiej HTTPS) i uniemożliwić dostęp zdalny.

Uzyskanie oświadczenia o bezpieczeństwie projektu

Dostawca powinien być w stanie przedstawić oświadczenie o bezpieczeństwie projektu, które będzie dowodem na cyberbezpieczeństwo każdego urządzenia podłączonego do sieci.

Dostęp do inteligentnych rozwiązań w systemie

W pełni inteligentnymi urządzeniami skomunikowanymi można nazwać te urządzenia, które łączą się z siecią za pomocą adresu MAC i stanowią kluczowy element architektury systemu. Urządzenia bez adresu MAC nie są inteligentne i nie można ich zidentyfikować, chronić ani nimi zarządzać na poziomie indywidualnym.

Ocena zgodności z RODO / brytyjską ustawą o ochronie danych osobowych

W 2018 roku w życie weszło rozporządzenie RODO, a także uaktualniona wersja brytyjskiej ustawy o ochronie danych osobowych z 1998 roku. W związku z tym należy upewnić się, czy produkty i systemy pozwalają na zachowanie zgodności z zapisami tych dokumentów.

O firmie Axis Communications

Axis umożliwia tworzenie mądrzejszego i bezpieczniejszego świata, tworząc sieć rozwiązań, które zapewniają wgląd w poprawę bezpieczeństwa i nowe sposoby prowadzenia biznesu. Jako lider branży sieciowych systemów wideo firma Axis oferuje produkty i usługi do monitoringu wideo i analityki, systemy kontroli dostępu, systemy domofonowe i rozwiązania audio. Axis zatrudnia ponad 3800 pracowników w ponad 50 krajach i współpracuje z partnerami na całym świecie, aby dostarczać rozwiązania dla klientów. Firma Axis została założona w 1984 roku i ma swoją siedzibę szwedzkim mieście Lund.

Więcej informacji o firmie Axis można znaleźć na stronie internetowej firmy pod adresem *axis.com*.